



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/670,783	09/27/2000	Joseph Andrew Mellmer	1909.2.74A	6748
1009	7590	05/02/2006	EXAMINER	
KING & SCHICKLI, PLLC 247 NORTH BROADWAY LEXINGTON, KY 40507			WOO, ISAAC M	
			ART UNIT	PAPER NUMBER
			2166	
DATE MAILED: 05/02/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/670,783

Applicant(s)

MELLMER ET AL.

Examiner

Isaac M. Woo

Art Unit

2166

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 February 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-58 and 90-101 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-58 and 90-101 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is in response to Applicant's Amendments, filed on February 13, 2006 have been considered but they are not persuasive.
2. Claims 2 and 59-89 are canceled. Claims 1, 3-58 and 90-101 are pending.

Response to Arguments

3. In response to Applicant's Remarks filed February 13, 2006, the following factual arguments are noted:

Dean et al (U.S. Patent No. 6,023,762) and/or French et al (U.S. Patent No. 5,794,228) does not disclose or suggest, "safe object containing multiple profiles accessed and administered exclusively by a single one of the multiple users at the exclusion of the system administrator, each profile including digital identity information provided by the single one of the multiple users and operable to be shared with other of the multiple users having other multiple different profiles accessible and administered exclusively by the other of the multiple users the sharing occurring exclusively upon initiation by the single one of the multiple users and storage of multiple user objects for multiple users".

However, examiner disagrees. Claimed invention is data access control system for multiple users with user profile. Dean teaches agent includes lookup table (410, fig. 5) checks caller objects that are used for control data access, according to category of caller, the category of caller is checked by user objects, such as, wife, boss, coworker, etc, that are multiple user profiles, are used as safe objects (col. 5, lines 23-56), and Dean discloses user personalize the type of data and services which can be accessed by each caller or category of caller through agent (col. 4, lines 47-65, col. 9, lines 1-10), which teaches that the safe objects are controlled by any single user who is not administrator and user provides digital identity information and each profile is shared with other multiple users. Dean teaches in order to share information with other multiple users, a user can configure access control according to each user's personal information (col. 4, lines 33-65). This sharing control is exclusively initiated by a single user who is not an administrator. Thus, the system of Dean teaches a user can do data access control without administrator authorization by configuring access control list by modifying personal information with respective target information. Therefore, Dean teaches claimed limitation that applicant argues above. French discloses data storage is shown, in fig. 3A-C, includes users' objects for users, (for example, user name, address age, gender, etc) for multiple users, in order to control data access control according to user profile information. Thus, combination of French with Dean provides Dean's system the capability of storing multiple user objects to effectively share and manage users' information with other users in multi-user-sharing network environment.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 90-101 are rejected under 35 U.S.C. 102(e) as being anticipated by Dean et al (U.S. Patent No. 6,023,762, hereinafter, "Dean").

With respect to claim 90, Dean discloses, defining vault for a storage of one or more safes digital identities, (each user database, 200-203, fig. 2, col. 4, lines 10-28 object, 401, fig. 4, lookup table provides authentication for authorizing access to user information), the vault (data storage means, col. 1, lines 49-52) including an access protocol layer (fig. 1, TCP/IP, col. 3, lines 27-65), an identity server layer (803, fig. 8, ID service, col. 8, lines 1-9) and an identity manager layer (805, 806, authorization service, fig. 8, col. 8, lines 1-39) and having access right granted to one or more system administrators (security level, col. 4, lines 33-40, authentication level, fig. 3) including management of the one or more safes of digital identities (fig. 3, authentication levels for authorizing access to user information, col. 4, lines 33-65) of one or more accounts

Art Unit: 2166

of end users (col. 4, lines 45-65, i.e., public, wife, boss, coworker, etc), the one or more safes of digital identities having multiple profile (fig.5, e.g., who am I , Dairy, personal information, etc) each with access right granted exclusively to the end users (fig. 5, col. 5, lines 40-67 to col. 6, lines 1-64, col. 4, lines 33-65, each personal information (profile) has different restrict access level controlled by look-up table for different requestor) via the one or more accounts (according to user ID, fig. 5, col. 5, lines 40-67 to col. 6, lines 1-13, col. 4, lines 33-65) including the exclusion of access rights of the one or more system administrators, (by each user without system administrators), the multiple profiles (fig. 5, col. 5, lines 40-67 to col. 6, lines 1-64, each personal information accessed by each category of user, i.e., public, wife, boss, etc) being shared amongst the end users at the exclusion of the one or more system administrators (fig. 5, col. 5, lines 40-65, each personal information accessed by each category of each end user, i.e., public, wife, boss, etc, each end user can access without system administrator).

With respect to claim 91, Dean discloses, access protocol layer includes one or more protocols selected from LDAP, XML, RPC-over-HTTP, XDAP or SMTP, see (col. 1, lines 11-21, TCP/IP internet).

With respect to claim 92, Dean discloses, server layer serves as an NDS access point, see (remote access service point, col. 1, lines 11-28).

With respect to claim 93, Dean discloses, server layer maintains access rights to the digital identities, see (fig. 3, authentication levels, col. 5, lines 2-22).

With respect to claim 94, Dean discloses, manager layer includes NDS authentication, see (remote access service authentication, col. 3, lines 45-60).

With respect to claim 95, Dean discloses, vault for secure storage of one or more safes of digital identity profiles, see (fig.5, e.g., who am I , Dairy, personal information, etc., col. 4, lines 47-65).

With respect to claim 96, Dean discloses, an identity server (106, fig.1, col. 3, lines 61-67), apportioned between a client (108, fig.1, user, col. 3, lines 45-48), a web server (col. 3, lines 28-37, internet service) and an identity server (106, fig.1, col. 3, lines 61-67).

With respect to claim 97, Dean discloses, an identity server, including servlets and applets, see (col. 3, lines 28-37, internet web service)

With respect to claim 98, Dean discloses, vault for secure storage of one or more safes digital identities, (each user database, 200-203, fig. 2, col. 4, lines 10-28 object, 401, fig. 4, lookup table provides authentication for authorizing access to user information), the vault (data storage means, col. 1, lines 49-52) having an access

Art Unit: 2166

protocol layer (fig. 1, TCP/IP, col. 3, lines 27-65), an identity server layer (803, fig. 8, ID service, col. 8, lines 1-9) and an identity manager layer (805, 806, authorization service, fig. 8, col. 8, lines 1-39) and having access right granted to one or more system administrators including management of the one or more safes of digital identities (401, fig. 4, lookup table provides authentication for authorizing access to user information, col. 4, lines 33-65, fig. 5, each personal information has different restrict access level controlled by look-up table for different requestor), (fig. 5, col. 5, lines 40-67, i.e., public, wife, boss, coworker, etc), the one or more safes of digital identities having multiple profile (fig.5, e.g., who am I , Dairy, personal information, etc) each with access right granted exclusively to the end users at location remote (fig. 5, i.e., public, wife, boss, coworker, etc) from the vault (data storage mean, col.1, lines 49-50), including the exclusion of access rights of the one or more system administrators, (by each user without system administrators), the multiple profiles (fig. 5, col. 5, lines 40-67 to col. 6, lines 1-13, each personal information accessed by each category of user, i.e., public, wife, boss, etc) being shared amongst the end users at the exclusion of the one or more system administrators (fig. 5, col. 5, lines 40-67, each personal information accessed by each category of each end user, i.e., public, wife, boss, etc, each end user can access without system administrator).

With respect to claim 99, Dean discloses, identity manager layer (803, fig. 8, ID service, col. 8, lines 1-9), client interface (108, fig. 1, user, col. 3, lines 41-49).

With respect to claim 100, Dean discloses, client application interface, see (108, user terminal, fig. 1, col. 3, lines 41-49).

With respect to claim 101, Dean discloses, the safe object containing at least one profile of the digital identity profiles administered by a user, see (fig. 5, col. 5, lines 40-65).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1 and 3-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dean et al (U.S. Patent No. 6,023,762, hereinafter, "Dean") in view of French et al (U. S. Patent No. 5,794,228, hereinafter, "French").

With respect to claim 1, Dean discloses, database (user databases, fig. 1, fig. 2, col. 28-45) including a vault (each user database, 200-203, fig. 2, col. 4, lines 10-28), the vault (data storage means, col. 1, lines 49-52) having access rights granted to a system administrator for management of the user objects (col. 4, lines 18-27, for

Art Unit: 2166

instance for personal information, personal preferences, bank or credit card details, personal medical details, etc), each of the user objects having a corresponding safe object (401, fig. 4, lookup table provides authentication for authorizing access to user information), (col. 4, lines 33-65, fig. 5, each personal information has different restrict access level controlled by look-up table for different requestor), the safe object containing multiple different profiles accessed (fig. 5, col. 5, lines 40-67 to col. 6, lines 1-64) and administered exclusively by a single one of the multiple users at the exclusion of the system administrator (col. 8, lines 65-67 to col. 9, lines 1-1-9, each user, without the system administrator, configures look-up table (safe object)), each profile (fig. 5, personal information, for instance, diary, personal information) including digital identity information provided by the single one of the multiple users (fig. 5, personal information, col. 5, lines 40-67) and operable to be shared with other of the multiple users having other multiple different profiles accessible (fig. 5, col. 5, lines 40-67 to col. 6, lines 1-25, for instance, Public can access information of "who am I" without access authentication to share "who am I" information) and administered exclusively by the other of the multiple users (each user, without the system administrator, configures look-up table (for safe object access)), the sharing occurring exclusively upon initiation by the single one of the multiple users, see (fig. 5, col. 5, lines 40-67 to col. 6, lines 1-25, a user configures look-up table for access control). Dean does not explicitly disclose, storage of multiple user objects for multiple users in lines 3-4. However, French discloses that data storage is shown, in fig. 3A-C, includes users' objects for users, (for example, user name, address age, gender, etc) for multiple users. Therefore, it would have been

Art Unit: 2166

obvious to a person having ordinary skill in the art at the time of the invention was made to modify Dean by incorporating storage of multiple user objects for multiple users with system of French. One having ordinary skill in the art at the time the invention was made would have been motivated to use such a combination because that would provide Dean's system the capability of storing multiple user objects to effectively share and manage users' information with other users in multi-user-sharing network environment.

With respect to claim 3, Dean discloses, safe object also contains at least one user-administered contact, each contact representing an entity outside the user's safe which receives controlled read access to digital identity information from at least one of the profiles, see (fig. 5, col. 5, lines 40-65, e.g., Public can access information of "who am I").

With respect to claims 4-7, Dean discloses, safe object also contains at least one drop box object, one application object with settings for an application, one view object, one access object, see (authentication level, fig. 3, every user object access control).

With respect to claims 8, Dean discloses, an identity server (106, fig.1, col. 3, lines 61-67) and a web server (col. 3, lines 28-37, internet service).

With respect to claims 9, Dean discloses, the identity server communicate using encrypted user names, see (col. 5, lines 23-39).

With respect to claim 10, Dean discloses, web server and the identity server are secured by a firewall, see (1001, firewall, fig. 10, col. 9, lines 10-32).

With respect to claim 11, Dean discloses, identity server appliance, see (106, server provider, fig. 1, col. 3, lines 28-45).

With respect to claims 12-13, Dean discloses, a zero-byte, installed client, see (108, user terminal, fig. 1, col. 43-47).

With respect to claim 14, Dean discloses, system comprises a provider model for access to the database, see (authentication level, fig. 3, every user object access control col. 4, lines 6-20).

With respect to claim 15, Dean discloses, abstract model offers a hierarchical storage system in a representation that includes a user, a container, and data, see (fig. 2, col. 4, lines 17-26).

With respect to claim 16, Dean discloses, programmatic interface to identity items and operations that correspond generally to directory service objects, see (col. 3, lines 28-42).

With respect to claim 17, Dean discloses, database includes multiple safe objects contained in a vault object, see (data storage means provides authentication level, col. 1, lines 49-60).

With respect to claim 18, Dean discloses, each vault object contains at least one user safe object, and objects contained by the safe objects are federated to provide controlled access between the vault servers, see (data storage means provides authentication level, col. 1, lines 49-60).

With respect to claim 19, Dean discloses, Universal Resource Identifier which specifies at least a protocol, a host, a path, and an object, see (fig.2, col. 4, lines 10-34).

With respect to claim 20, Dean discloses, digital business card application object having a corresponding profile object which includes digital identity information provided by the user, see (fig. 3, col. 5, lines 5-22).

With respect to claim 21, Dean discloses, one user to receive updated profile information of another user using a link to the database partitioned directory services database, see (col. 5, lines 40-67).

With respect to claim 22, Dean discloses, partitioned directory services database, see (fig. 2, col. 4, lines 18-33).

With respect to claim 23, Dean discloses, account creation service which creates a new account for a user based on a template, see (fig. 6, col. 7, lines 24-42).

With respect to claim 24, Dean discloses, administrative tool to manage and maintain safe objects, see (fig. 5, col. 5, lines 40-52).

With respect to claim 25, Dean discloses, schema management service which permits an administrator to at least view a directory service schema, see (fig. 5, col. 5, lines 40-65).

With respect to claim 26, Dean discloses, batch account creation service which creates several accounts at one time, see (col. 9, lines 1-9).

With respect to claim 27, Dean discloses, install service which permits one to install and configure an identity server, see (106, server provider, fig. 1, col. 3, lines 28-45).

With respect to claim 28, Dean discloses, backup and restore service which allows one to backup and restore at least one safe object, see (fig. 6, col. 7, lines 24-42).

With respect to claim 29, Dean discloses, safe advisor service which allows one to verify the integrity of a safe object, see (col. 9, lines 1-9).

With respect to claim 30, Dean discloses, legal recovery tool which recovers digital identity information for forensic use, data demoralization service which facilitates data transformation on database fields, see (col. 4, lines 17-26).

With respect to claims 31, Dean discloses, data denormalization service which facilitates data transformation on database fields, see (col. 3, lines 28-67, by database management system).

With respect to claim 32, Dean discloses, rules service, see (col. 3, lines 28-67).

With respect to claim 33, Dean discloses, identity server to register interest in and be notified of changes in the database, see (col. 3, lines 28-67).

With respect to claim 34, Dean discloses, event service which allows an identity server to register interest in and be notified of changes in the database, see (col. 3, lines 28-67).

With respect to claim 35, Dean discloses, process to verify information gathered from a user registration form, see (fig.3, col. 5, 1-24, user ID is used for verification).

With respect to claim 36, Dean discloses, profile discovery and publishing service which allows users to publish at least a portion of their profile information, see (fig. 6, col. 7, lines 24-42).

With respect to claim 37, Dean discloses, allows a user to have the service fill in at least part of an online form with information from one of the user's profile objects, see (col. 9, lines 1-31).

With respect to claim 38, Dean discloses, form conversion service which assists a webmaster in converting existing forming to standardized field names, see (col. 3, lines 27-67).

With respect to claim 39, Dean discloses, install service which installs servlets on a web server, see (col. 3, lines 27-67).

With respect to claim 40, Dean discloses, identity exchange service for portions of a privacy protection protocol, see (1001, firewall, fig. 10, col. 9, lines 11-55, col. 3, lines 27-67).

With respect to claim 41, Dean discloses, chat service which sets up chat rooms so users can communicate with each other in real time, see (fig. 6, col. 7, lines 24-42).

With respect to claim 42, Dean discloses,, presence service which lets users specify where they are and allows them to discover another user's presence information, see (col. 9, lines 1-31).

With respect to claim 43, Dean discloses, anonymous remailer service which allows users to choose different email addresses for different profiles, see (fig. 6, col. 7, lines 24-42).

With respect to claim 44, Dean discloses, anonymous browsing service which allows a user to browse a network in an anonymous fashion to prevent sites from collecting user identity information, see (col. 4, lines 17-26).

With respect to claim 45, Dean discloses, infomediary service which facilitates creating an infomediary, see (col. 5, lines 40-67 to col. 6, lines 1-25).

With respect to claim 46, Dean discloses, tracking IP addresses in order to selectively publish the last known IP address of a user, see (col. 1, lines 11-29).

With respect to claim 47, Dean discloses, underlying directory service and an underlying file system in order to enforce access controls on web pages published by users, see (col. 1, lines 31-65).

With respect to claim 48, Dean discloses, email services, encodes contact relationship information in the user's email address, see (col. 1, lines 31-67).

With respect to claim 49, Dean discloses, contact relationship information in the user's email address, see (fig. 6, col. 8, lines 28-48).

With respect to claim 50, Dean discloses, profiles to filter email sent to the user, see (col. 1, lines 31-67).

With respect to claim 51, Dean discloses, determining whether a user logging in at a third party web site is registered as a user of the system, see (604, fig. 6, col. 8, lines 15-34, log-in requests).

With respect to claim 52, Dean discloses, logging the user into the system if the user is registered, and a means for registering the user and logging the user in if the user was not registered, see (604, fig. 6, col. 8, lines 15-34, log-in requests).

With respect to claim 53, Dean discloses, registering the user and logging the user in comprises a means for capturing user login information for the third party web site, see (fig. 6, col. 8, lines 28-48).

With respect to claim 54, Dean discloses, user digital identity information is only made available to a partner site if the user has flagged the information as public, see (fig. 6, col. 8, lines 19-34).

With respect to claim 55, Dean discloses, icon provides a transaction history, see (col. 5, lines 40-67).

With respect to claim 56, Dean discloses, user authentication mechanism, see (604, fig. 6, col. 7, lines 14-46, agent requests user authentication information).

With respect to claim 57, Dean discloses, launch point for launching application, see (fig. 6, col. 8, lines 15-34).

With respect to claim 58, Dean discloses, non-repudiation feature whereby an administrator cannot change a user password and then log on as the user, see (fig. 6, col. 7, lines 14-46).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any

Art Unit: 2166

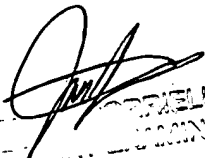
extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Isaac M. Woo whose telephone number is (571) 272-4043. The examiner can normally be reached on 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hosain T. Alam can be reached on (571) 272-3978. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


ISAAC M. WOO
PATENT EXAMINER

IW
April 26, 2006